一种基于超混沌的图像零水印算法 *

张海涛，张思博，

(辽宁工程技术大学 软件学院，辽宁 葫芦岛 125105)

摘 要：超混沌系统有着密钥空间大、初值敏感的特性，又对其公式进行了改进，具有一定的优越性。针对已有的零水印算法鲁棒性差、安全性低的问题进行了研究，提出了一种基于超混沌的图像零水印算法，首先利用 Chen 三维超混沌系统对水印信息进行加密预处理，通过解析各个位平面在分解后对图像的影响，将载体图像中的最低有效位初始化为零；采用块均值二值量化的方法进行特性提取；最后通过对加密水印与 Anorld 置乱后的特征矩阵进行异或处理得到零水印。仿真攻击实验及与以往零水印算法对比表明，该算法在保持鲁棒性良好的同时，能够抵御噪声攻击、滤波攻击、压缩攻击、剪切攻击等多种攻击。

关键词：超混沌加密；Chen 混沌系统；鲁棒性；零水印

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2018.07.0437

Research on zero watermaking algorithm for hyper-chaos-based image

Zhang Haitao, Zhang Sibo

(*College of Software Liaoning Technical University*, *Huludao* 125105, *China*)

Abstract: Hyperchaotic system has certain advantages because of its characteristics of sercret key space and sensitivity to initial value. Aiming at the low computation efficiency and poor security of the existing Zero watermarking algorithm, this paper proposed a zero watermark algorithm based on hyperchaotic system. Firstly the algorthm realizes the encryption pretreatment of watermarking information taking advantage of the large key space and sensitivity of initial value of the Chen hyper-chaos system. And then analyzing the influence of each bit plane on the image, least significant bit of the image carrier is initialized to zeros to extract the feature matrix using of block mean binary quantization method. Finally, Arnold scrambled characteristics matrix and hyper-chaotic encrypted binary watermarking are executed for xor operation to construct a zero watermarking. The simulation attack experiment and comparison with the precious zero watermark algorithm show that the algorithm in this paper can resist noise attack, filter attack, compression attack and shear attack while maintaining better robustness.

Key words: hyper-chaos encryption; Chen system; robustness; zero watermarking

0 引言

随着互联网和信息多媒体技术的迅速发展，人们的生活变得更加快捷，人们可以通过 QQ、微博同其他人进行信息的交流，各种图片、视频在互联网上不断被观看和传递，在这个信息爆炸的时代，科技作为一把双刃剑在带给人们生活便利的同时，也存在着巨大的隐患，一些不法分子通过对互联网上的信息例如图片、视频进行盗窃、窜改、传播来为自己牟取利益，这些行为轻则损害版权使用者的合法利益，重则给社会给国家造成不可挽回的损失，在网络传输中有一系列的不确定因素，例如噪声的干扰、图像失真、丢失传输包等，这些都会造成接受方无法确定收到的数据的真实性以及完整性，所以，数字图像版权的保护问题显得格外重要[1-2]。

1989 年，混沌映射产生密码序列的思想被 Matthews 首次提出[3],混沌动力系统对初始条件非常敏感，不同的初始条件，通过复杂的混沌动力学行为，会产生截然不同的混沌序列。混沌系统有确定的公式，但是初始值细微的变化会导致混沌序列的不同走向，在这种看似确定实为随机的动力学行为下，难以预测的混沌加密序列又给算法增添了一种保障。混沌系统随着维度的增加，其动力学行为会更加复杂，更难以预测，Chen 混沌系统是经典的三维混沌系统，它具有系统结构复杂、产生的序列多、且随机性更强，方便设计加密系统，它多参数、多初值的特点又使整个加密系统多了密钥空间大的优点[4~6]。通过混沌系统所产生的混沌序列对水印加密,会提高水印的鲁棒性、安

收稿日期：2018-07-25；**修回日期：**2018-09-15　　**基金项目：**总装备部装备预研基金项目；辽宁省自然科学基金面上项目（2017054042）

作者简介：张海涛（1974-），男，黑龙江绥化人，教授，博士，主要研究方向为高光谱图像压缩、图形图像处理（lntuzht@163.com）；张思博（1994-），男，硕士研究生，主要研究方向为图形图像处理.

全性。

现阶段，利用混沌对水印加密的算法有很多，兀旦晖,郑恩让等人在针对图像水印鲁棒性的问题上，提出了一种基于混沌映射 logistic 和 Arnold 二次加密的图像水印的算法研究[7]；季诺然,吕晓琪等人针对现行数字水印算法中抗几何攻击能力弱以及嵌入水印信息容量差的问题,提出一种 Contourlet 变换下 QR 码与混沌加密相结合的彩色图像水印算法[8]；曲长波、于智龙等人结合二维混沌系统、SVD 和位平面技术共同构造零水印信息，提出了一种基于脊波变换域的鲁棒零水印算法[9]；曲长波、吴德阳等人利用 Arnold 置乱和特征矩阵构造零水印信息，提出了一种基于 Curvelet-DSVD 和视觉密码相结合的强鲁棒零水印算法[10]。以上几种算法均采取的是利用低维混沌映射去对水印图像进行加密,水印图像的鲁棒性以及安全性都得到了提高，本文将 chen 经典三位混沌系统进行降维为一维混沌系统，利用其产生的混沌序列对水印图像进行加密，在对各个平面分解之后对于图像影响的解析，找到载体图像的最低有效位，并将其初始化为零，采用块均值量化的方法对其进行特征提取，把特征矩阵进行 Arnold 变换后与加密水印退休那个异或得到零水印，通过一系列的仿真实验可以得到，本文算法的拥有良好的鲁棒性，以及能够抵御噪声攻击、剪切攻击、滤波攻击以及压缩攻击等多种攻击。

1 本文算法

1.1 水印的预处理

由于考虑到一维的混沌映射的动力学行为相比较于高维混沌系统而言较为简单，本文算则利用 Chen 经典三维混沌系统对本文图像水印进行加密处理，以往的研究表明，Chen 混沌系统是一个非常容易用电路实现的三阶系统，可用于实现更高安全性的加密系统[4~6]。

本身 chen 混沌系统对于初始值的微小改动是十分敏感的，通过式（2）的降维模型将其降为一维后，其中 H，C 值的作用是用来放大混沌系统对于初始值的敏感性的，这会使新的一维混沌系统比 Chen 混沌系统本身对初始值的改动更具敏感性，Chen 混沌系统的动力学方程可描述如下：

$$\begin{cases} dx/dt = a(y-x) \\ dy/dt = (c-a)x - xz + cy \\ dz/dt = xy - bz \end{cases} \quad (1)$$

将上式混沌系统按照下式降为一维混沌映射：

$$L_k = floor(H\sqrt{x_k y_k + y_k z_k + x_k z_k} + C)$$

$$k=0,1,2,\ldots\ldots,N\times N \quad (2)$$

其中:x_k，y_k，z_k 是 chen 混沌系统的三个状态变量在第 k 时刻的值，H，C 为控制参数，混沌系统对于初始值是具有敏感性的，文本想要将 chen 混沌系统降为一维，就是想让这个改造后的一维混沌映射的敏感性更强，因此在式（2）中的因子 H 是用来大幅度地放大这种敏感性，而因子 L 是用来小幅度地放大这种敏感性。

本算法选择大小为 N×N 的二值水印图像 $W(i,j)$，其中 $0<i\le N$，$0<j\le N$。初始值为 x_0、y_0 和 z_0，这三个初始值将作为密钥 K1 保存起来。以三个初始值为起点，在 chen 混沌系统的迭代作用下产生三组混沌序列 x(k)、y(k)和 z(k)，其中 $k=1,2\ldots N\times N$。将三维混沌序列进行降维处理，为保证降维后的序列具有更好的超混沌特性和良好的扩散均匀度[11]，选取式（2）的参数降维模型。

设所选参数 $N=256$，经过降维公式(2)处理后的超混沌序列如图 1 所示。

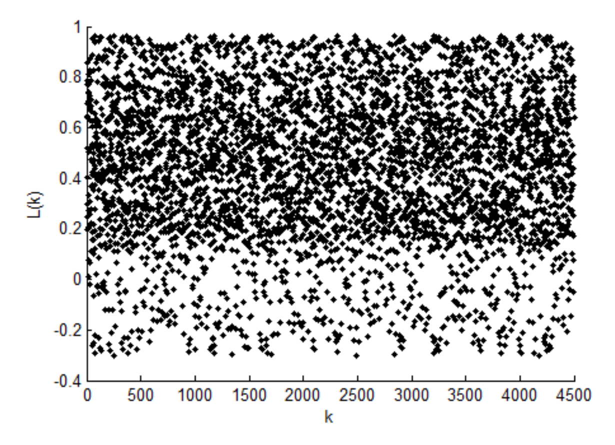


图 1 三维超混沌序列经降维后的序列

本文选取的实验对象为二值图像，一组混沌序列无法满足对二维图像加密，所以首先要对 L(k)序列进行升维为二维矩阵 LL(k)，通过式(3)(4)最终得到加密后的水印图像。

$$J(i,j)=\begin{cases}1 & LL(i,j)>ml \\ 0 & LL(i,j)<=ml\end{cases} \quad ml=mean(LL) \quad (3)$$

$$C(i,j)=W(i,j)\oplus J(i,j) \quad (4)$$

其中:ml 为升维后的二维矩阵的均值，当二位矩阵中的点的值大于均值 ml 时,矩阵 J(i,j)赋值为 1，反之，赋值为 0，经过二值量化处理后，得到矩阵 J(i,j)。由公式(4)将矩阵 J(i,j)与而至水印图像进行异或处理后得到加密后的二维水印数组 C(i,j)。

图 2 为水印加密预处理框图。

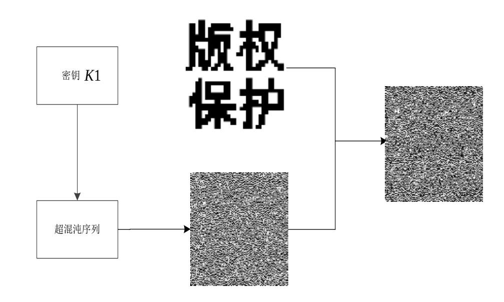


图 2 水印加密预处理框图

1.2 特征矩阵的提取以及零水印的构造

图像特征提取是构造零水印的重要的一环，它决定着算法的鲁棒性的算法的好坏，本文将 256×256 的 Lena 灰度图像按照式(5)进行位平面分解，如图 3(a)~(i)所示。

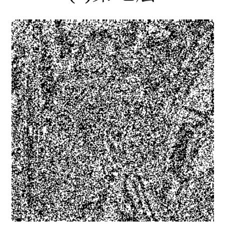
$$S_k(i,j)=B_k(S(i,j))=\begin{cases}1, \mathrm{mod}(floor(S(i,j)/2^{k-1}),2)=1 \\ 0, \mathrm{mod}(floor(S(i,j)/2^{k-1}),2)=0\end{cases} \quad (5)$$

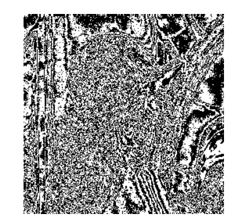

(a)原始图像

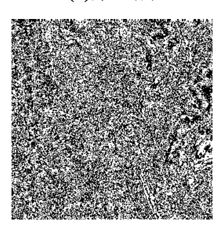

(b)MSB 层

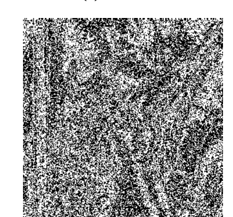

(c)第七层

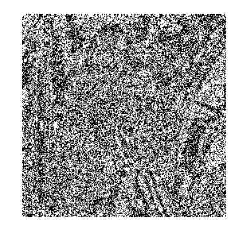

(d)第六层


(e)第五层


(f)第四层


(g)第三层


(h)第二层


(i)LSB 层


(j)LSB 层置零后 Lena 图像

图 3　Lena 图像的位平面分解图

由图 3 可以看出，Lena 灰度图像位平面分解的各个层面中，MSB 层的轮廓最为清晰，随后是第六层和第七层，随着平面位的下降，像素逐渐变得不规则，在后面的几幅图像中可以直观地看到像素的分布毫无规律可循，这是因为图像的可视性权重的大小是由位平面的高低决定的，可视性会随着为平面的升高而占比增加，图像所包含的信息量也会随着增加[12]。

通过对图 3(a)~(i)的分析，可以发现 LSB 作为最低有效位，它包含的信息量非常少，类似一些随机的信号，为了改善原始图像的纹理信息丢失情况，本文算法对 LSB 进行了初始化为零的操作。如图 3(j)为 Lena 灰度图像 LSB 层初始化为零之后的图像，通过计算，图 3(j)的 PSNR 的值为 51.12 dB,明显要大于 35 dB,故可判断其与原始图像的差异是微小的，提取过程中纹理信息的丢失是较小的，特征矩阵的提取以及零水印的构造的流程图如图 4 所示。

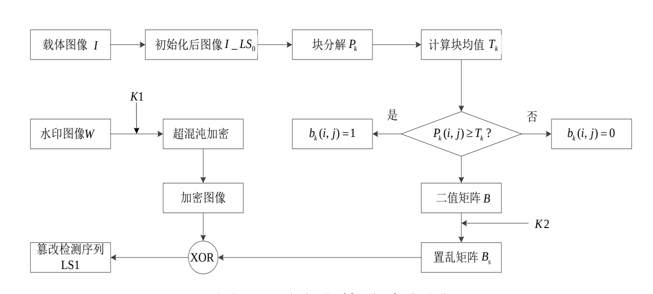


图 4　零水印构造流程图

本文算法选取 N×N 的原始图像 I 作为水印嵌入载体，具体构造零水印的步骤如下：

a)通过对原始载体图像 I 的最低有效位初始化为零，得到 I_LS_0。

b)对所得到的图像 I_LS_0 做分块处理，大小为 m×m,用 P_k 标记每个子块，只是单纯的标号。

c)通过式(6)来计算每个子块的均值 T_k。

$$T_k=\frac{1}{m^2}\sum_{i=1}^{m}\sum_{i=1}^{m}P_k(i,j)\qquad i,j=1,2,\ldots,m\quad(6)$$

d)把每一个子块中的像素值与其所处子块做比较，构造一个大小为 N×N 的矩阵 B,其中 b_k 为每块中每个像素点的像素值。

e)对矩阵 B 进行次数为 K 次的 Arnold 变换，得到置乱后的矩阵 B_S.

f)将步骤 e)中得到置乱矩阵 B_S 与加密后的水印序列 C 进行异或操作得到 LSI 序列，长度为 N×N。

2　仿真实验以及安全性分析

在实验部分的所有实验均在 MatlabR2010b 的实验环境下进行，试验中所选取的原始图像为 256×256 的经典 lena 图像，水印信息采取二值图像版权保护四个字，实验中，在实验中的水印加密阶段，混沌系统初始值以及参数取 x0=0.123、y0=0.321、z0=0.231,H =30、C=1.27,将以上数据作为密钥 K1 保存，Arnold 置乱二值矩阵的次数为 75，将此置乱次数作为密钥 K2 进行保存，实验中所使用的原始图像与水印图像如图 5 所示，其中(a)为原始图像，(b)为水印图像。


(a)原始载体图像

版权
保护

(b)水印图像

图 5　原始载体图像和水印图像

2.1　算法抵御攻击的性能分析

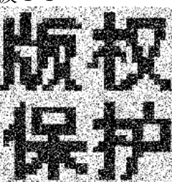
2.1.1 压缩攻击和滤波攻击

压缩攻击和滤波攻击是最为常见的攻击方式，压缩图像是为了减少图像在传输的过程中由于数据量过大，会对信道产生过大的压力，从而影响传输的速率；滤波是给图像去噪的操作，主要是为了过滤图像中高频的成分，在这两个过程中都会损失

图像的像素。在实验中，压缩攻击选取的是 JEPG 压缩,其中选取压缩质量因子 60、70、80 的三种情况，滤波的模板选择了 3*3 和 5*5 两种对原始载体图像进行测试，采取 NC 值对前后水印的差距做出客观的评估,滤波攻击测试结果图如图 6 所示，压缩攻击测试结果图如图 7 所示，结果如表 1 所示。




(a)中值滤波 3*3

(b)中值滤波 5*5

图 6　中值滤波载体图像和提取水印




(a) JPEG 压缩质量因子为 80




(b) JPEG 压缩质量因子为 70




(c) JPEG 压缩质量因子为 60

图 7　JPEG 压缩载体图像和提取水印

如图 6、7 所示，随着滤波攻击模板的扩大，原始载体图像质量有所下降，但从水印图像来看并没有受到太大的影响，图片中的字样依旧清晰可见；压缩攻击方面，随着压缩质量因子的减小，原始载体图像和水印图像都收到了轻微的影响，但是这种影响在可以接受的范围内，所以，从实验效果图来看，本文算法对于滤波攻击和压缩攻击有一定程度的抵抗能力。

如表 1 所示，水印 NC 的值随着滤波模板的增大而减小，在两种模板中的测试值的值都在 0.85 之上，在压缩攻击方面，水印 NC 的值随着压缩因子的增大而增大，三次测试结果的值也在 0.87 之上，所以说，本文算法在受到一定程度的滤波攻击或者压缩攻击时仍能保持一种良好的鲁棒性。

表 1　攻击后得到的水印 NC 值

攻击方式	中值滤波		JPEG 压缩		
压缩质量因子与滤波模板选择	3*3 模板	5*5 模板	质量因子 60	质量因子 70	质量因子 80
NC 值	0.8966	0.8502	0.8795	0.8894	0.9008

2.1.2 噪声攻击

噪声攻击是一种较为常见的图像攻击方式，图像在传输的过程中都会收到噪声的干扰，高斯噪声和椒盐噪声为两种非常普遍的噪声攻击，本次实验采用高斯噪声与椒盐噪声两种攻击方式和不同的强度对原始载体图像进行测试，如图 8、9 为高斯噪声和椒盐噪声攻击下的原始图像和提取水印图像。


(a)高斯噪声 0.001


(b)高斯噪声 0.002


(c)高斯噪声 0.003

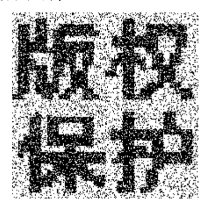

(d)椒盐噪声 0.01

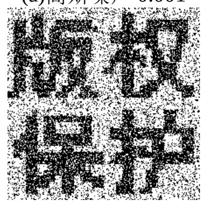

(e)椒盐噪声 0.02

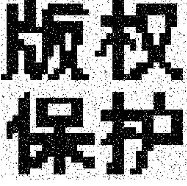

(f)椒盐噪声 0.03

图 8　噪声攻击后载体图像


(a)高斯噪声 0.001


(b)高斯噪声 0.002

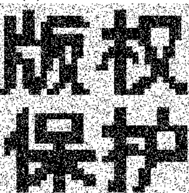

(c)高斯噪声 0.003



(d)椒盐噪声 0.01



(e)椒盐噪声 0.02



(f)椒盐噪声 0.03

图 9　噪声攻击后提取水印图像

如图 7、8 所示，无论是高斯噪声还是椒盐噪声，随着噪声

的增大，图片的质量变得越来越差，提取的水印图像的清晰度也逐渐降低，但是水印图像的基本轮廓大致都能看得出，其中的“版权保护”依然可以轻易分辨，所以，本算法能够抵御一定范围的高斯噪声和椒盐噪声。

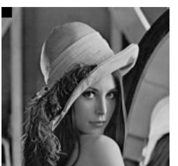
表 2　噪声攻击后得到的水印 NC 值

噪声攻击类型	攻击强度	NC 值
高斯噪声	0.001	0.8508
	0.002	0.7645
	0.003	0.7388
椒盐噪声	0.01	0.9461
	0.02	0.9157
	0.03	0.8952

如表 2 所示，无论是高斯噪还是椒盐噪声，随着噪声强度的增大，NC 值不断减小，当高斯噪声的噪声强度为 0.003 时，虽然 NC 值与椒盐噪声攻击的 NC 值差距较大，但是 NC 值仍能保持在 0.73 以上，当椒盐噪声的噪声强度为 0.03 时，NC 值仍保持在 0.89 以上，所以，本文算法能够抵御一定程度的高斯噪声和椒盐噪声的攻击。

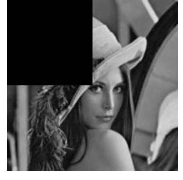
2.1.3 剪切攻击

剪切攻击是一种常见的攻击方式，与其他攻击方式比较来说更为直观，它是直接对图像进行任意规则的剪切，从而破坏掉图像信息，在这一部分的实验中，一共选取了图片左上角、图片中心、图片右下角三个剪切部位，每个部位分别采取了四种不同程度的剪切面积，图 10、11 分别为原始载体图像裁剪后的效果图以及水印提取的图像的效果图。

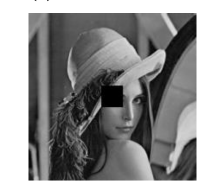

(a)左上角剪切 1/16


(b)左上角剪切 1/8


(c)左上角剪切 1/4


(d)左上角剪切 1/2


(e)中心剪切 1/16


(f)中心剪切 1/8


(g)中心剪切 1/4


(h)中心剪切 1/2


(i)右下角剪切 1/16


(j)右下角剪切 1/8


(k)右下角剪切 1/4


(l)右下角剪切 1/2

图 10　剪切攻击后的载体图像

(a)左上角剪切 1/16　(b)左上角剪切 1/8　(c)左上角剪切 1/4

(d)左上角剪切 1/2　(e)中心剪切 1/16　(f)中心剪切 1/8

(g)中心剪切 1/4



(h)中心剪切 1/2

(i)右下角剪切 1/16

(j)右下角剪切 1/8　(k)右下角剪切 1/4　(l)右下角剪切 1/2

图 11　剪切攻击后提取的水印图像

由图 11 可以看出剪切攻击无论是从左上角、中心还是右下角对图像进行攻击并没有什么太大的差别，但是无论是哪一个部位，随着剪切面积的增大，所提取的水印图像就变得越模糊，尤其是剪切面积从 1/4 变化到 1/2 的手，前后两张水印图像模糊程度差异较大，但是剪切面积最大为 1/2 的时候，所提取的水印图像仍能非常清楚的辨别图片中的字体，所以说，本文算法可以很好的抵御大强度的剪切攻击。除了效果图，还计算了每张提取的水印图像的 NC 值 如表 3 所示。

表 3　剪切攻击后得到的水印 NC 值

剪切位置	剪切尺寸	NC 值
左上角	1/16	0.9982
	1/8	0.9916
	1/4	0.9679
	1/2	0.8743
中心	1/16	0.9973
	1/8	0.9911
	1/4	0.9667
	1/2	0.8686
右下角	1/16	0.9972
	1/8	0.9909
	1/4	0.9909
	1/2	0.8642

由表 3 可以看出 NC 值和效果图的结果一致对应，NC 值随着剪切面积的增大而减小，最低时的 NC 值在 0.86 以上，这

表明本文算法具有面对一定程度的剪切攻击，能够保持良好的鲁棒性。

2.1.4 图像篡改攻击

在这一部分，主要测试本文算法对于篡改攻击的抵御效果，主要从内容删除、文本添加和拷贝粘贴三个方面进行，图 12~14 分别为内容删除、文本添加、拷贝粘贴的实验效果图。



(a) (b)

图 12 内容删除攻击



(a) (b)

图 13 添加文本攻击



(a) (b)

图 14 复制粘贴窜改攻击

如图 12 中，(a)为被内容删除攻击的原始载体图像，(b)是对图(a)的水印提取的效果图；如图 13 中，(a)为被添加文本攻击的原始载体图像，(b)是对(a)的水印提取的效果图；如图 14 中，(a)为被拷贝粘贴攻击的原始载体图像，(b)为对(a)的水印提取的效果图。

从上述几幅图象可以看出，本文算法对于内容删除、添加文本、拷贝粘贴攻击均具有良好的鲁棒性，在载体图像收到以上几种攻击之后，提取的水印图像仍然清晰可见，从客观评价的角度来说，表 4 给出了几种窜改攻击后的图像的 PSNR 值和 NC 值。

表 4 窜改图像 PSNR 值和提取水印 NC 值

攻击类型	PSNR	NC
拷贝粘贴攻击	26.4652	0.9911
文本添加攻击	24.1951	0.9864
内容删除攻击	26.4821	0.9833

由表 4 可以看出在三种篡改攻击下的水印提取图像的 NC 值均在 0.98 之上，故本文算法在面对篡改攻击时具有极好的鲁棒性。

2.2 水印加密安全性分析

在这一部分主要是对水印加密算法的安全性的测试，本文水印加密算法运用了 Chen 混沌系统和 Arnold 变换对水印图像和特征矩阵进行加密和置乱，在整个加密过程中，共产生两个密钥分别为 K1、K2，其中的值均为系统初始化的取值，想要提取水印图像必须依赖两个密钥，在这一部分载体图像选取 Lena 和 Boat 两幅二值图像作为载体图像进行测试，如图 3.11 为密钥不同时的水印提取效果。

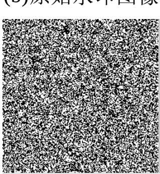


(a)原始载体图像 lena

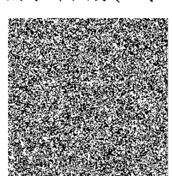


(b)原始水印图像

(b)提取的水印图像(K1、K2 正确)



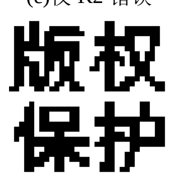
(d)仅 K1 错误



(e)仅 K2 错误

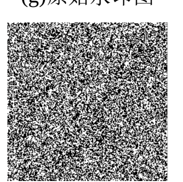


(f)原始载体图像 Boat

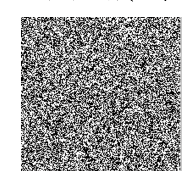


(g)原始水印图

(h)提取的水印图像(K1、K2 正确)



(i)仅 K1 错误



(j)仅 K2 错误

图 15 不同密钥下提取出的水印图像

由图 15 可以看出，在密钥 K1、K2 中的任何一个出现错误时，提取的水印信息类似于随机噪声，不能对水印图像进行成功的提取，所以，在不得到密钥的情况下，是不可能对水印图像进行正确的提取。

2.3 算法性能比较

在这一部分，测试本文算法与其他算法在鲁棒性上的对比效果，选取噪声攻击、剪切攻击、滤波攻击三种类型的攻击，并且采取不同的强度对算法的鲁棒性进行测试，如表 5 为测试结果。

表 5 算法鲁棒性评价(NC 值)

攻击类型	攻击强度	文献[13]	文献[14]	本文算法
高斯噪声	0.001	0.5022	0.5024	0.8058
	0.002	0.5006	0.5017	0.7645
	0.003	0.4964	0.4988	0.7388
中值滤波	3*3	0.6612	0.6209	0.8966
	5*5	0.5927	0.5660	0.8502
剪切攻击	中心剪切 1/16	0.9778	0.9967	0.9973
	中心剪切 1/4	0.9685	0.9790	0.9667

从表 5 可以看出，在抵御高斯噪声和中值滤波攻击的方面的能力,本算法要优于文献[13，14],在剪切攻击的方面，本算法要稍逊于文献[13，14],文献[11]在构造特征矩阵的方法是采用置乱图像的最低有效位，由于 LSB 算法对于噪声攻击和几何攻击表现较为脆弱，在被攻击后所提取的水印图像和原始的水印图像存在差异性。文献[14]采用的不是零水印这种无损的嵌入方式，而是一种有损的嵌入方式，通过水印来代替载体图像的最低有效位，这样虽然可以获得一定的鲁棒性，但是会破坏载体图像。本文算法采取零水印这种无损的嵌入方式，不会使原始载体图像发生任何变化，在构造特征阶段采取 LSB 置零后分块像素值和块均值的大小关系，在受到攻击时，块均值不会有太大的变化，鲁棒性好，因此在与文献[13，14]比较下，本算法具有更好的水印提取效果。

3　结束语

本文提出了一种基于超混沌的图像零水印算法，采用零水印技术这种无损的方式，在不改变原始载体图像的情况下，提高了鲁棒性，在水印加密阶段采用 Chen 高维混沌系统结合 Arnold 变换完成，提高了水印的安全性，通过一系列的攻击实验以及和其他算法的比较，可以得出，本文算法能够抵御噪声攻击、滤波攻击、压缩攻击等多种攻击，并且具有良好的水印提取效果。

参考文献：

[1] Seitz J. Digital watermarking for digital media [M]. London: Information Science Publishing, 2005: 1-30.

[2] Cox I, Miller M, Bloom J, *et al.* Digital Watermarking and Steganography [M]. San Francisco, California: Morgan Kaufmann Publishers, 2007: 15-56.

[3] Matthews R A J. On the derivation of a chaotic encryption algo-rithm [J]. Cryptologia, 1989, 13 (1): 29-42.

[4] Chen Guanrong, Dong Xiaoning. From Chaos to order methodologies, perspectives and applications [J]. World Scientific, 1998, 24 (16): 760.

[5] Ueta T, Chen Guanrong. Bifurcation analysis of Chen's equation [J]. International Journal of Bifurcation and Chaos, 2000, 10 (8): 1917-1931.

[6] Yassen M T. Chaos control of Chen chaotic dynamical system [J]. Chaos, Solitons &Fractals, 2003, 15 (2): 271-283.

[7] 兀旦晖，郑恩让. 基于混沌 Logistic 和 Arnold 二次加密的图像水印算法研究 [J]. 计算机测量与控制，2017, 25 (04): 193-196. (Wu Danhui, Zheng Enrang. Research of encryption algorithm of image watermarking based on logistic and arnold of chaos [J] , Computer Measurement & Control, 2017, 25 (04): 193-196.)

[8] 季诺然，吕晓琪，谷宇，等. 基于 QR 码与混沌加密的 Contourlet 域彩色图像盲水印算法 [J]. 包装工程, 2017, 38 (15): 173-178. (Ji Nuoran, Lyu Xiaoqi, Gu Yu, *et al.* Blind watermarking algorithm for color image in contourlet domain based on QR code and chaotic encryption [J] , Packaging Engineering, 2017, 38 (15): 173-178)

[9] 曲长波，于智龙，李栋栋. 基于分块 FRIT-SVD 的鲁棒零水印算法 [J]. 计算机工程与科学, 2018, 40 (06): 1005-1016. (Qu Changbo, Yu Zhilong, Li Dongdong. A robust zero-watermarking algorithm based on the block FRIT-SVD [J] , Computer Engineering and Science, 2018, 40 (06): 1005-1016)

[10] 曲长波，吴德阳. 基于 Curvelet-DSVD 和视觉密码的强鲁棒零水印算法 [J/OL]. 计算机应用研究，2019, 36 (3) . [2018-09-13]. http://kns. cnki. net/kcms/detail/51. 1196. TP. 20180209. 1115. 064. html. (Qu Changbo, Wu Deyang. Strong robust zero-watermarking algorithm based on Curvelet-DSVD and visual cryptography [J] , Application Research of Computers, 2019, 36 (3) . [2018-09-13]. http://kns. cnki. net/kcms/detail/51. 1196. TP. 20180209. 1115. 064. html.)

[11] 杨晋霞，鞠杰，邵峰. 基于超混沌加密的半脆弱音频水印算法 [J]. 计算机应用与软件, 2014, 31 (11): 295-298. (Yang Jinxia, Ju Jie, Shao Feng. Semi-fragile audio watermarking algorithm based on hyper-chaos encryption [J] , Computer Applications and Software, 2014, 31 (11): 295-298.)

[12] 姚雪. 一种基于位平面和 HVS 的信息隐藏算法研究 [D]. 葫芦岛：辽宁工程技术大学，2014. (Yao Xue. Research on information hiding algorithm based on bit-plane and HVS [D]. Huludao: Liaoning Technical University, 2014)

[13] 吴伟民，丁冉，林志毅，等. 基于混沌的医学图像窜改定位零水印算法 [J]. 计算机应用研究, 2014, 31 (12): 3685-3688. (Wu Weimin, Ding Ran, Lin Zhiyi, etal. Chaos-based zero-bit watermarking scheme for medical image tamper location [J] , Application Research of Computers, 2014, 31 (12): 3685-3688.)

[14] Sanjay R, Raman B. A chaotic system based fragile watermarking scheme for image tamper detection [J]. International Journal of Electronics and Communications, 2011, 65 (10): 840-847.